UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/940,982	08/29/2001	Takashi Endo	NIT-295	5993

24956 7590 02/20/2007

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/940,982	ENDO ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 November 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 08 November 2006 has been entered.

2. By the above submission, Claim 1 has been amended. No claims have been added or canceled. Claims 1-8 are currently under examination in the present application.

Response to Amendment

3. The supplemental amendment received on 24 November 2006 was not filed during a period of suspension of action as provided for in 37 CFR 1.111(a)(2)(ii) and is therefore not entered as a matter of right. Further, the supplemental amendment will not be entered because it adds new claims and therefore is not clearly limited to the responses provided for by 37 CFR 1.111(a)(2)(i).

Response to Arguments

4. Applicant's arguments filed 08 November 2006 and 16 October 2006 have been fully considered but they are not persuasive.

Claims 1-8 were rejected under 35 U.S.C. 103(a) as unpatentable over applicant admitted prior art in view of Jaffe et al, US Patent 6510518.

Regarding independent Claim 1, Applicant first argues that "using the terminology of the present specification, Jaffe maps input data D1 to obtain data H1" (page 8 of the response received 08 November 2006). First, the Examiner notes that the term "map" or "mapping" does not, in fact, seem to appear in the present specification, contrary to Applicant's assertion. Further, Applicant asserts that "One would seem to map the input data D1, for example, before disturbing D1 with disturbance data Y1, or perhaps one would disturb D1 with the disturbance data Y1 and then map the resulting data to obtain H1 with a constant hamming weight" (pages 8-9 of the response received 08 November 2006, emphasis added). However, the Examiner notes that this assertion is merely a broad supposition or allegation by Applicant of what would result from the combination, which would result from bodily combining the steps of Jaffe with the steps of the admitted prior art, rather than the modifications of the admitted prior art that would be suggested to one of ordinary skill by the teachings of Jaffe. However, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the

Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). The Examiner also notes that the above assertion does not provide any citations to the prior art in support of the suppositions or allegations. Applicant further argues that Jaffe does not teach mapping twice, and that if one "were to map the disturbed data... the disturbance data itself would not have a constant hamming weight" (page 9 of the response received 08 November 2006). The Examiner again notes that Applicant does not provide any citations to the prior art in support of these arguments, which merely amount to allegations.

Further, the Examiner notes that it was previously stated that the teachings of Jaffe would reasonably suggest to one of ordinary skill in the art to use a constant Hamming weight representation for all data within a system such as the one admitted as prior art (see, for example, page 3 of the Office action mailed 08 May 2006, the summary of the interview conducted on 12 September 2006, or the advisory action mailed 30 October 2006). Therefore, the Examiner believes that one of ordinary skill would be motivated to represent not only the disturbance data XI and the processed disturbance data XO using constant Hamming weight representations, but also the input data D1, the transformed data H1, the processed transformed data H2, and the processed data D2, in order to protect all of that data against side channel attacks (noting Jaffe, column 2, lines 44-48). The Examiner further notes that Jaffe does not suggest a "mapping" as a specific operation to be performed as part of processing, but

rather as a type of representation of the binary values of TRUE and FALSE (see the general description at Jaffe, column 4, line 55-column 5, line 30).

Regarding Claim 2, Applicant argues that the admitted prior art does not teach that the processing of the data for disturbance used in the inverse transformation is the predetermined processing (see pages 11-12 of the response received 16 October 2006). However, the Examiner believes that it is implicit from the language on page 21 ("a result of processing the data for disturbance") and from prior art Figure 4 (noting step 405, "transformed data processing method"; 406, "transformed data H2"; and 408, "transformed data for disturbing X1o") that the processing performed on the data and the disturbance data is the same predetermined processing.

Regarding Claim 3, Applicant argues that the cited portion of Jaffe does not disclose each bit having a logic value of 1 or 0 at a probability of 50%, arguing that variable s_8 is not disturbance data but instead an intermediate variable and that it is initialized to a known state (see page 12 of the response received 16 October 2006). However, the Examiner notes that the other cited portion of the art (Jaffe, column 8, lines 41-45) specifically define the representation such that half of the bits have a logic value of 1 and the other half have a logic value of 0. The Examiner further notes column 5, lines 12-18, where the representations "(01, 10), (0101, 10101), and (0110, 1001)" in which each bit has a logic value of 1 or 0 at probability 50%.

Regarding Claim 4, Applicant argues that the admitted prior art does not disclose that XI is processed by any particular process to obtain XO (see pages 12-13 of the response received 16 October 2006). Again, the Examiner believes that it is implicit

from the language on page 21 ("a result of processing the data for disturbance") and from prior art Figure 4 (noting step 405, "transformed data processing method"; 406, "transformed data H2"; and 408, "transformed data for disturbing X1o") that the processing performed on the data and the disturbance data is the same predetermined processing. The Examiner further notes that combination with Jaffe further suggests the claimed limitations of the generated XI and XO having a constant Hamming weight (for example, at column 4, line 55-column 5, line 30).

Regarding Claim 5, Applicant argues that the cited portion of the admitted prior art does not disclose disturbance data storage means or disturbance data select means as claimed (see page 13 of the response received 16 October 2006). However, the Examiner believes that the cited portion does at least disclose the limitation that disturbance data processing is carried out to process the selected XI in order to generate XO (see again page 21, lines 6-8 and Figure 4). Further, the Examiner believes that Jaffe discloses means for storing and selecting candidates for data to be used in various calculations (see, for example, column 16, lines 15-32).

Regarding Claim 6, Applicant's arguments, set forth in the response received 16 October 2006, were addressed in the advisory action mailed 30 October 2006. To summarize, the Examiner believes that Jaffe does disclose random initialization (column 7, lines 62-64), and more specifically means for generating numbers each having Hamming weight equal to half the number of bits in the generated number (see Figures 1 and 4; see also column 5, lines 12-18); bit inversion means (column 8, lines 41-45;

Figure1, step 150; Figure 4, step 450); and bit concatenation means (Figure 1, steps 110-120; Figure 4, steps 410-420).

Regarding Claim 7, Applicant argues that Jaffe does not suggest random number generation, computation or examination of Hamming weights, or generation of new random numbers and assurance of constant Hamming weight (see page 14 of the response received 16 October 2006). However, the Examiner believes that Jaffe does disclose random number generation (column 7, lines 62-64), and the Examiner again notes that the representations noted in the cited portion (column 4, line 55-column 5, line 30) guarantee a constant Hamming weight. The Examiner further notes that Jaffe discloses that the Hamming weights of various variables can be computed and examined (see Figure 1; column 8, lines 25-29 and 46-65).

Regarding Claim 8, Applicant argues that Jaffe does not disclose random number generation, and specifically does not disclose generation of constant Hamming weight or constant fractional bit count random numbers (see pages 14-15 of the response received 16 October 2006). However, the Examiner believes that Jaffe does disclose random number generation (column 7, lines 62-64) and generation of partial random numbers where each portion has a uniform constant Hamming weight and a fraction of the bit count of a final random number (Figure 1, step 115; Figure 4, step 415). Jaffe further discloses data concatenation means (Figure 1, steps 110-120; Figure 4, steps 410-420)

Therefore, for the reasons detailed above, the Examiner maintains the rejection as set forth below.

Specification

5. The objection to the disclosure for informalities is withdrawn in light of the amendments to the specification. Applicant's cooperation is again requested in correcting any other errors of which applicant may become aware in the specification.

Terminal Disclaimer

6. As noted in the advisory action mailed 30 October 2006, the terminal disclaimer filed on 16 October 2006 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of Patent No. 6,615,354 has been reviewed and is accepted. The terminal disclaimer has been recorded.

Double Patenting

7. The rejection of Claims 1-8 on the ground of nonstatutory obviousness-type double patenting is withdrawn in light of the above-noted terminal disclaimer.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant admitted prior art in view of Jaffe et al, US Patent 6510518.

In reference to Claim 1, Applicant admits as prior art an apparatus including a data transform means transforming input data by using disturbance data to generate transformed data, a transformed data processing means for carrying out predetermined processing on the transformed data to generate processed transformed data, and a data inverse transform means for carrying out inverse transformation processing on the processed transformed data using processed disturbance data to generate processed data (see page 21, lines 1-12 of the present application). However, Applicant admits that such prior art does not explicitly disclose that the disturbance data and the processed disturbance data have a constant Hamming weight.

Jaffe discloses that data used in cryptographic processing can be represented using a constant Hamming weight representation (column 4, line 55-column 5, line 30). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of the prior art to include constant

Hamming weight data, in order minimize the information leaked from cryptosystems by power consumption fluctuations (see Jaffe, column 2, lines 44-48).

In reference to Claim 2, Applicant admits that the prior art further discloses that the processed disturbance data can be generated by carrying out the predetermined processing on the disturbance data (page 21, lines 6-8 of the present application; see also prior art Figure 4).

In reference to Claim 3, Jaffe further discloses that each bit has a logic value of 1 or 0 at a probability of 50% (see the table at column 9, noting the representations s_8; see also column 8, lines 41-45, and column 5, lines 12-18).

In reference to Claim 4, Applicant admits that the prior art further discloses generating processed disturbance data by carrying out the predetermined processing on the disturbance data (page 21, lines 6-8 of the present application; see also prior art Figure 4, and Jaffe, column 4, line 55-column 5, line 30).

In reference to Claim 5, Applicant further admits and Jaffe further discloses a disturbance data storage means, disturbance data select means, and that processing is carried out on the disturbance data in order to generate the processed disturbance data (page 21, lines 6-8 of the present application, and prior art Figure 4; Jaffe, column 16, lines 15-32).

In reference to Claim 6, Jaffe further discloses means for generating random numbers each having a Hamming weight equal to half the numbers of bits include in the random number (column 7, lines 62-64; see Figures 1 and 4; see also column 5, lines 12-18), means for inverting bits of data (column 8, lines 41-45; Figure1, step 150; Figure

4, step 450), and means for concatenating a random number with data output by the means for inverting (Figure 1, steps 110-120; Figure 4, steps 410-420).

In reference to Claim 7, Jaffe further discloses a random number generation means (column 7, lines 62-64), a Hamming weight computation means (see Figure 1; column 8, lines 25-29 and 46-65), a Hamming weight examination means (see Figure 1; column 8, lines 25-29 and 46-65), and a constant Hamming weight assurance means (see column 4, line 55-column 5, line 30, where the representations guarantee a constant Hamming weight).

In reference to Claim 8, Jaffe further discloses random number generation means to generate partial random numbers with uniform constant Hamming weights and bit count each equal to a fraction of a final random number (Figure 1, step 115; Figure 4, step 415); means to generate random numbers until a sum of bit counts is equal to the final bit count (column 7, lines 62-64); and means for concatenating the partial random numbers (Figure 1, steps 110-120; Figure 4, steps 410-420)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ZAD
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER